



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/944,192	08/30/2001	Hideaki Watanabe	09792909-5126	1206

26263 7590 06/22/2006

SONNENSCHN NATH & ROSENTHAL LLP
P.O. BOX 061080
WACKER DRIVE STATION, SEARS TOWER
CHICAGO, IL 60606-1080

EXAMINER

HENEGHAN, MATTHEW E

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 06/22/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.		Applicant(s)	
	09/944,192		WATANABE ET AL.	
	Examiner		Art Unit	
	Matthew Heneghan		2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 07 April 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-40 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-40 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 30 August 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 16 March 2006 has been entered.

2. In response to the previous office action, Applicant has amended claims 1, 12, 21, 29, 36, and 40. Claims 1-40 have been examined.

Claim Objections

3. Claims 1, 12, 21, 29, and 40 are objected to because of the following informalities: In each claim, the limitation "wherein said encrypted sampling information generates using a public key certificate..." is improperly phrased and difficult to understand. It is being presumed that each claim is meant to read "wherein said encrypted sampling information is generated using a public key certificate..." as per claim 36. Appropriate correction is required.

4. Claims 12, 29, and 36 are objected to because of the following informalities:

Each claim lacks a transitional phrase. It is being presumed that the limitations are being recited in an open-ended manner after “by” in claim 12 and “wherein” in claims 29 and 36.

Appropriate correction is required.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claim 40 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 40 recites a program from a program providing medium. Applicant's specification discloses that a “program providing medium” may be a transmission medium such as a network (see Specification, p. 22, first full paragraph), which comprises intangible signals. Since the claim therefore encompasses intangible matter, it is non-statutory.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

6. Claims 1-40 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Claims 1, 12, 21, 29, 36, and 40 recite that the encrypted sampling information is generated using a public key. Applicant has not pointed out support for this limitation in the specification; moreover, Applicant's specification only appears to suggest that the sampling information is to be encrypted using a session key (see Specification, p. 98, lines 12-15), which is different from the public key.

All other claims depend from rejected claims above, and include all the limitations of those respective claims, thereby rendering those dependent claims as failing to comply with the written description requirement.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

7. Claims 1, 9, 21, 28, 36, 38 and 40 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,256,737 to Bianco et al.

Regarding claim 1, Bianco discloses a person authentication system comprising:
an entity for executing person authentication (computer 208 containing biometric device object 722),

wherein said entity acquires a template from a person identification certificate storing template information (biometric template) including said template and generated by a third-party agency (biometric server 104) serving as a person identification certificate authority (col. 24, lines 21-31),

All information sent from the server, including the template, is encrypted (see column 56, lines 62-65) and must necessarily be decrypted before being used (see column 55, lines 32-35) and

executes person authentication on the basis of the acquired template (col. 24, lines 37-39).

Bianco further discloses that all transactions both with the server and with the biometric identity device are encrypted using public key cryptography and processed using the public key system engine (see column 56, lines 40-65).

Regarding claim 9, Bianco teaches all the limitations of claim 1, and further teaches

that said entity is a user device serving as a data processing apparatus including data accessible by a user identified by said person identification certificate (computer 208; col. 11, line 66, through col. 12, line 22), and

that said user device compares a template, which is acquirable from the person identification certificate acquired from said person identification certificate authority, with sampling information provided by the user (col. 24, lines 21-43, and col. 25, lines 31-50),

and said user device allows the user to start accessing said user device, provided that said template and said sampling information match with each other (col. 24, lines 40-56).

Regarding claims 21 and 28, these are a method version of the claimed system discussed above (claims 1 and 9, respectively), wherein all claim limitations have been addressed. Thus, for the reasons provided above, such claims also are anticipated.

Regarding claims 36 and 38, this is an information-processing-apparatus version of the claimed system discussed above (claims 1 and 4), wherein all claim limitations

have been addressed. Thus, for the reasons provided above, such claims also are anticipated.

Regarding claim 40, Bianco discloses a program-providing-medium version (see column 14, lines 62-67) of the claimed system discussed above (claim 1), wherein all claim limitations have been addressed. Thus, for the reasons provided above, such a claim also is anticipated.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

8. Claims 1-3, 8, 10, 21-23, 36, 37, 39 and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,310,966 to Dulude et al. in view of Schneier, "Applied Cryptography," 1996, pp. 31-32.

Regarding claim 1, Dulude discloses a person authentication system comprising:
an entity for executing person authentication (receiver station 42),
wherein said entity acquires a template from a person identification certificate storing template information (biometric certificate 68) including said template and generated by a third-party agency (registration authority 34) comprising encrypted

information (a digital signature) serving as a person identification certificate authority (col. 4, lines 12-65, and col. 6, lines 1-17 and 32-34). Received user sampling information is also optionally encrypted (see column 5, lines 63-67). A receiving unit that receives the encrypted template and encrypted sampling information is shown (see figure 5, inputs 46 and 68). The system executes person authentication on the basis of the acquired decrypted template (col. 6, lines 58-65, and col. 7, lines 33-44).

Dulude does not disclose the manner by which the user sampling information is encrypted, or whether a common unit is to be used for decrypting the encrypted template and the encrypted sampling information.

Schneier discloses the use of public-key cryptography in all communications between a computer and those with whom it communicates, where any user who wishes to communicate with a particular computer uses the same public key, which is then decrypted using the receiver's private key. Since all incoming communications are being encrypted using the same algorithm, a common decryptor would therefore be used on the receiving end. Schneier further suggests that this is done so that someone listening in cannot recover the message (see Section 2.5).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the invention of Dulude by using public-key cryptography for all communications to the receiver, as disclosed by Schneier, so that someone listening in cannot recover the message.

Regarding claim 2, Dulude further teaches that the person identification certificate authority includes a digital signature written by said person identification

certificate authority (biometric certificate 68 contains digital signature 22; Fig. 2; col. 4, lines 55-65).

Regarding claim 3, Dulude further teaches that
said person identification certificate authority verifies the identification of a person requesting a person identification certificate to be issued (col. 5, lines 16-25),
acquires a template serving as person identification data of said person requesting the person identification certificate to be issued (col. 4, lines 25-32), and
generates a person identification certificate storing template information including said template (col. 4, lines 55-65).

Regarding claim 8, Dulude further teaches that
said entity is a service provider which provides services to a user identified by said person identification certificate (receiving section 42 is service provider; col. 8, lines 34-45, incorporating Vaeth, US 6035,402; see Vaeth, col. 6, lines 5-26), and
that said service provider compares a template (registration biometric data 72), which is acquirable from the person identification certificate acquired from said person identification certificate authority (col. 4, lines 55-65, and col. 6, lines 32-34), with sampling information provided by the user (transaction biometric data 46) and starts providing services with the user, provided that said template and said sampling information match with each other (col. 7, lines 33-67).

Regarding claim 10, Dulude further teaches that
said template (registration biometric data) is composed any one of: biometric information of a person; non-biometric information; any combination of two or more of

said biometric information and said non-biometric information; and a combination of any of said information and a password (template composed of biometric information; col. 4, lines 26-32 and 55-57).

Regarding claims 21-23, these are a method version of the claimed system discussed above (claims 1-3, respectively), wherein all claim limitations have been addressed. Thus, for the reasons provided above, such claims also are obvious.

Regarding claims 36 and 37, these are an information-processing-apparatus version of the claimed system discussed above (claims 1 and 2), wherein all claim limitations have been addressed. Thus, for the reasons provided above, such claims also are obvious.

Regarding claim 39, Dulude further teaches that

said information processing apparatus compares a template (registration biometric data 72), which is acquirable from the person identification certificate acquired from said person identification certificate authority (col. 4, lines 55-65, and col. 6, lines 32-34), with sampling information provided by the user (transaction biometric data 46) and starts providing services with the user, provided that said template and said sampling information match with each other (col. 7, lines 33-67).

Regarding claim 40, since Dulude's invention is being executed using computerized equipment, the claimed program must be embodied on a computer-readable medium. This is a program-providing-medium version of the claimed system discussed above (claim 1), wherein all claim limitations have been addressed. Thus, for the reasons provided above, such a claim also is obvious.

9. Claims 6 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,310,966 to Dulude et al. in view of Schneier, "Applied Cryptography," 1996, pp. 31-32 further in view of U.S. Patent No. 6,035,402 to Vaeth et al.

Dulude further teaches that said entity is any one of a service provider which provides services to a user identified by said person identification certificate, a user device accessed by a user identified by said person identification certificate, and said person identification certificate authority (receiving section 42 is service provider; col. 8, lines 34-45, incorporating by reference Vaeth, US 6,035,402; see Vaeth, col. 6, lines 5-26).

10. Claims 5, 7, 25 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dulude in view of Schneier, "Applied Cryptography," 1996, pp. 31-32 as applied to claims 1 and 21 above and further in view of Hughes ("Digital Envelopes and Signatures," InstantDoc #2698, WindowsITPro, September 1996).

Regarding claim 5, Dulude and Schneier teach all the limitations of claim 1, but does not explain the further limitation that said person identification certificate authority stores said template in said person identification certificate after encrypting said template.

However, Hughes teaches a method for securing the transmission of a message wherein both the encryption of the message and the digital certificate (signature) for the

message sender are employed concurrently for the purpose of providing both privacy and authentication (page 3, paragraph 5).

Therefore, it would be obvious to a person of ordinary skill in the computer art at the time the invention was made to modify the system of Dulude and Schneier with the teaching of Hughes such that said person identification certificate authority stores said template in said person identification certificate after encrypting said template, particularly where the biometric database 66 which stores the biometric certificate 68 is accessed over a network connection (col. 5, lines 33-44 and col. 6, lines 32-43). One would be motivated to do so in order to ensure both privacy and authentication in transmission of the biometric certificate over a network.

Regarding claim 7, Dulude and Schneier teach all the limitations of claim 1, but does not explain the further limitation that, when transmitting said person identification certificate to said entity, said person identification certificate authority transmits a template which is stored in said person identification certificate, as an encrypted template which is decryptable only by said entity to which said person identification certificate is to be transmitted.

However, Hughes teaches a method for securing the transmission of a message wherein both the encryption of the message and the digital certificate (signature) for the message sender are employed concurrently for the purpose of providing both privacy and authentication (page 3, paragraph 5), and wherein the encrypted message is decryptable only by the entity to which the certificate is to be transmitted (page 2, paragraph 2).

Therefore, it would be obvious to a person of ordinary skill in the computer art at the time the invention was made to modify the system of Dulude and Schneier with the teaching of Hughes such that, when transmitting said person identification certificate to said entity, said person identification certificate authority transmits a template which is stored in said person identification certificate, as an encrypted template which is decryptable only by said entity to which said person identification certificate is to be transmitted, particularly where the biometric database 66 which stores the biometric certificate 68 is accessed over a network connection (col. 5, lines 33-44 and col. 6, lines 32-43). One would be motivated to do so in order to ensure both privacy and authentication in transmission of the biometric certificate over a network.

Regarding claims 25 and 26, this is a method version of the claimed system discussed above (claims 5 and 7), wherein all claim limitations have been addressed. Thus, for the reasons provided above, such claims also would have been obvious.

11. Claims 4, 11, and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bianco as applied to claims 1 and 21 above in view of Diffie et al., "Authentication and Authenticated Key Exchanges," Designs, Codes and Cryptography, Kluwer Academic Publishers, 1992.

Regarding claim 4, Bianco teaches all the limitations of claim 1, and further teaches that said person identification certificate authority transmits the person identification certificate to said entity (col. 24, lines 21-32).

Although Bianco teaches that the transmission of the certificate between said person identification certificate authority and said entity is encrypted using an asymmetric public key protocol (col. 55, lines 29-57, and col. 56, lines 52-65), Bianco does not explain that in the process of acquiring the person identification certificate from said person identification certificate authority, said entity performs mutual authentication between said entity and said person identification certificate authority, and said person identification certificate authority transmits the person identification certificate provided that said mutual authentication is successfully completed.

However, Diffie teaches a method of two-party mutual authentication wherein the parties exchange digital signatures (page 9, first paragraph) in addition to their public cryptographic keys for the purpose of enhancing security by assuring that each of the parties exchanging a public key is authentic and not an imposter (page 2, paragraph 3).

Therefore, it would be obvious to a person of ordinary skill in the computer art at the time the invention was made to modify the system of Bianco with the teaching of Diffie such that in the process of acquiring the person identification certificate from said person identification certificate authority, said entity performs mutual authentication between said entity and said person identification certificate authority, and said person identification certificate authority transmits the person identification certificate provided that said mutual authentication is successfully completed. One would be motivated to do so in order to enhance network security by assuring that each of the parties exchanging a public key is authentic and not an imposter.

Regarding claim 11, Bianco teaches all the limitations of claim 1, and further teaches

that said entity and said person identification certificate authority have an encryption processing unit, respectively, (col. 56, lines 58-65).

But Bianco does not explain that when data is transmitted between said entity and said person identification certificate authority, mutual authentication is performed, a data-transmitting party generates a digital signature and adds it to data to be transmitted, and a data-receiving party verifies the digital signature.

However, Diffie teaches a method of two-party mutual authentication wherein the parties exchange digital signatures (page 9, first paragraph) in addition to their public cryptographic keys for the purpose of enhancing security by assuring that each of the parties exchanging a public key is authentic and not an imposter (page 2, paragraph 3).

Therefore, it would be obvious to a person of ordinary skill in the computer art at the time the invention was made to modify the system of Bianco with the teaching of Diffie such that when data is transmitted between said entity and said person identification certificate authority, mutual authentication is performed, a data-transmitting party generates a digital signature and adds it to data to be transmitted, and a data-receiving party verifies the digital signature. One would be motivated to do so in order to enhance network security by assuring that each of the parties exchanging a public key is authentic and not an imposter.

Regarding claim 24, this is a method version of the claimed system discussed above (claim 4), wherein all claim limitations have been addressed. Thus, for the reasons provided above, the claim also is obvious.

12. Claims 12-14, 16-18, 20, 29-31, 33, and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,930,804 to Yu et al. in view of U.S. Patent No. 6,310,966 to Dulude et al. further in view of Schneier, "Applied Cryptography," 1996, pp. 31-32.

Regarding claim 12, Yu discloses a person authentication system comprising:
a person identification certificate authority (authentication center 24 containing biometric server 42) which acquires a template (stored biometric data),
executes person authentication on the basis of said acquired template (col. 11, lines 5-13), and

issues a verification certificate, provided that said person authentication is successfully passed (col. 11, lines 66-67, and col. 12, lines 33-43).

But Yu does not explain that the person identification certificate authority acquires the template from a person identification certificate storing template information including said template.

However, Dulude teaches an authentication system wherein a template (registration biometric data 20) is stored within a person identification certificate (biometric certificate 68; Fig. 2; col. 4, lines 55-65; col. 5, lines 33-35) for the purpose of facilitating increased security and accuracy in the authentication of electronic

transactions by binding the biometric identification of consumers with digital certificates (col. 3, lines 28-34).

Therefore, it would be obvious to a person of ordinary skill in the computer art at the time the invention was made to modify the system of Yu with the teaching of Dulude such that the person identification certificate authority acquires the template from a person identification certificate storing template information including said template. One would be motivated to do so in order to facilitate increased security and accuracy in the authentication of electronic transactions by binding the biometric identification of consumers with digital certificates.

Yu and Dulude also do not disclose the manner by which the user sampling information is encrypted, or whether a common unit is to be used for decrypting the encrypted template and the encrypted sampling information.

Schneier discloses the use of public-key cryptography in all communications between a computer and those with whom it communicates, where any user who wishes to communicate with a particular computer uses the same public key, which is then decrypted using the receiver's private key. Since all incoming communications are being encrypted using the same algorithm, a common decryptor would therefore be used on the receiving end. Schneier further suggests that this is done so that someone listening in cannot recover the message (see Section 2.5).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the invention of Yu and Dulude by using public-

key cryptography for all communications to the receiver, as disclosed by Schneier, so that someone listening in cannot recover the message.

Regarding claim 13, the modified invention of Yu, Dulude, and Schneier is relied upon as applied to claim 12, and Yu further teaches that the verification certificate issued by said person identification certificate authority includes a digital signature written by said person identification certificate authority (Yu, col. 12, lines 36-57).

Regarding claim 14, the modified invention of Yu, Dulude, and Schneier is relied upon as applied to claim 12, and Yu further teaches that

said person identification certificate authority acquires a template serving as person identification data of said person requesting the person identification certificate to be issued (col. 9, lines 54-63).

Yu, Dulude, and Schneier as heretofore cited do not explicitly explain that said person identification certificate authority verifies the identification of a person requesting a person identification certificate to be issued and that said person identification certificate authority generates a person identification certificate storing template information including said template.

However, Dulude teaches an authentication system wherein said person identification certificate authority verifies the identification of a person requesting a person identification certificate to be issued (col. 5, lines 15-25) and wherein a person identification certificate authority (registration authority 34) generates a person identification certificate (biometric certificate 68) storing template information (registration biometric data 20) including said template (Fig. 2; col. 4, lines 55-65) for the

purpose of facilitating increased security and accuracy in the authentication of electronic transactions by binding the biometric identification of consumers with digital certificates (col. 3, lines 28-34).

Therefore, it would be obvious to a person of ordinary skill in the computer art at the time the invention was made to modify the modified invention of Yu, Dulude, and Schneier as applied to claim 12 with the further teaching of Dulude such that said person identification certificate authority verifies the identification of a person requesting a person identification certificate to be issued and that said person identification certificate authority generates a person identification certificate storing template information including said template. One would be motivated to do so in order to facilitate increased security and accuracy in the authentication of electronic transactions by binding the biometric identification of consumers with digital certificates.

Regarding claim 20, the modified invention of Yu, Dulude, and Schneier is relied upon as applied to claim 12, and Yu further teaches that said template is composed of any one of: biometric information of a person; non-biometric information; any combination of two or more of said biometric information and said non-biometric information; and a combination of any of said information and a password (biometric data; col. 9, lines 54-67, and col. 10, lines 61-67).

Regarding claims 29-31, this is a method version of the claimed system discussed above (claims 12-14), wherein all claim limitations have been addressed. Thus, for the reasons provided above, such claims also would have been obvious.

Regarding claim 16-18, 33, and 34, Yu further discloses that authentication information for the session is sent to the user by the server. This information may be a session certificate that is valid for the user session (see column 12, lines 9-42).

13. Claims 19 and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,930,804 to Yu et al. in view of U.S. Patent No. 6,310,966 to Dulude et al. further in view of Schneier, "Applied Cryptography," 1996, pp. 31-32 as applied to claims 12 and 29 and further in view of U.S. Patent No. 6,298,153 to Oishi.

Yu, Dulude, and Schneier do not disclose the deletion of certificates after their use.

Oishi discloses the use of one-time certificates (which are discarded after use) that are authenticated with a digital signature, in order to retain the anonymity of a user (see column 18, lines 25-43).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Yu, Dulude, and Schneier by using one-time certificates, as disclosed by Oishi, in order to retain the anonymity of a user.

14. Claims 15 and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,930,804 to Yu et al. in view of U.S. Patent No. 6,310,966 to Dulude et al. further in view of Schneier, "Applied Cryptography," 1996, pp. 31-32 as applied to claims 12 and 29 above in view of Diffie et al., "Authentication and

Authenticated Key Exchanges,” Designs, Codes and Cryptography, Kluwer Academic Publishers, 1992.

Yu discloses a transaction with the biometric server, but does not disclose a mutual authentication in the accessing of that server.

Diffie teaches a method of two-party mutual authentication wherein the parties exchange digital signatures (page 9, first paragraph) in addition to their public cryptographic keys for the purpose of enhancing security by assuring that each of the parties exchanging a public key is authentic and not an imposter (page 2, paragraph 3).

Therefore, it would be obvious to a person of ordinary skill in the computer art at the time the invention was made to modify the system of Yu, Dulude, and Schneier with the teaching of Diffie such that in the process of acquiring the person identification certificate from said person identification certificate authority, said entity performs mutual authentication between said entity and said person identification certificate authority, and said person identification certificate authority transmits the person identification certificate provided that said mutual authentication is successfully completed. One would be motivated to do so in order to enhance network security by assuring that each of the parties exchanging a public key is authentic and not an imposter.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the

Art Unit: 2134

unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

15. Claims 1-5, 7, 10, 12-15, 20-26, 29-32, 36-38, and 40 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1, 9, 10, and 40 of U.S. Patent No. 7,059,516 in view of Schneier, "Applied Cryptography," 1996, pp. 31-32.

Regarding claims 1, 12, 21, 29, and 36, the '516 patent discloses the acquisition of a certificate including a template from a certificate authority (see claim 1, second limitation); the template is encrypted (see claim 1, fifth limitation); the received template is compared with the received sampling information from the user (see claim 1, fifth limitation), thus constituting a receiving unit; extraction of the template from the certificate, which necessarily requires decryption (see claim 1, fifth limitation).

The '516 patent does not disclose that the user sampling information is encrypted, or whether a common unit is to be used for decrypting the encrypted template and the encrypted sampling information.

Schneier discloses the use of public-key cryptography in all communications between a computer and those with whom it communicates, where any user who wishes to communicate with a particular computer uses the same public key, which is then decrypted using the receiver's private key. Since all incoming communications are being encrypted using the same algorithm, a common decryptor would therefore be used on the receiving end. Schneier further suggests that this is done so that someone listening in cannot recover the message (see Section 2.5).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the invention of the '516 patent by using public-key cryptography for all communications to the receiver, as disclosed by Schneier, so that someone listening in cannot recover the message.

As per claims 2, 13, 22, 30, and 37, the certificate contains the digital signature of the certifying authority (see claim 1, fourth limitation).

As per claims 3, 14, 23, and 31, a certificate is generated (see claim 1, seventh limitation).

As per claims 4, 15, 24, 32, and 38, mutual authentication is performed (see claim 9).

As per claims 5 and 25, the template is stored in the certificate in encrypted form.

As per claims 7 and 26, since the template is encrypted with the public key of the personal authentication system, it can only be decrypted by the personal authentication system.

As per claims 10 and 20, biometric or non-biometric information may be used (see claim 10).

As per claim 40, the method is executable on a program providing medium (see claim 24).

16. Claims 1, 2, 5-7, 10, 12, 13, 20-22, 25-27, 30, 36, 37, 39, and 40 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1, 2, 5, 12, and 24 of copending Application No. 09/944,424 in view of Schneier, "Applied Cryptography," 1996, pp. 31-32.

As per claim 1, 12, 21, 29, and 36, a certificate is acquired from a certificate authority having an encrypted template (see claims 1 and 5); the template and user information that has been received are compared (see preamble of claim 1); since the template is encrypted, it must necessarily be decrypted in order to be used.

The '424 application does not disclose that the user sampling information is encrypted, or whether a common unit is to be used for decrypting the encrypted template and the encrypted sampling information.

Schneier discloses the use of public-key cryptography in all communications between a computer and those with whom it communicates, where any user who wishes to communicate with a particular computer uses the same public key, which is

Art Unit: 2134

then decrypted using the receiver's private key. Since all incoming communications are being encrypted using the same algorithm, a common decryptor would therefore be used on the receiving end. Schneier further suggests that this is done so that someone listening in cannot recover the message (see Section 2.5).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the invention of the '424 application by using public-key cryptography for all communications to the receiver, as disclosed by Schneier, so that someone listening in cannot recover the message.

As per claim 2, 13, 22, 30, and 37, a digital signature written by the authority is disclosed (see claim 2).

As per claim 5 and 25, the template is stored in the certificate (see claim 1).

As per claim 6, 27, and 39, the system may be a service provider (see claim 12).

As per claims 7 and 26, since the template is encrypted with the public key of the personal authentication system, it can only be decrypted by the personal authentication system.

As per claims 10 and 20, biometric or non-biometric information may be used (see claim 12).

As per claim 40, the method is executable on a program providing medium (see claim 24).

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

17. Claims 1-5, 7, 10, 12-15, 20-26, 29-32, 36-38, and 40 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1, 3, 9, 11, and 27 of copending Application No. 09/944,501 in view of Schneier, "Applied Cryptography," 1996, pp. 31-32.

As per claim 1, 12, 21, 29, and 36, a certificate is acquired from a certificate authority having an encrypted template; the template and user information that has been received are compared (see preamble of claim 1); since the template is encrypted, it is decrypted in order to be used (see claim 1). Public keys are used (see claim 3).

The '501 application does not disclose that the user sampling information is encrypted, or whether a common unit is to be used for decrypting the encrypted template and the encrypted sampling information.

Schneier discloses the use of public-key cryptography in all communications between a computer and those with whom it communicates, where any user who wishes to communicate with a particular computer uses the same public key, which is then decrypted using the receiver's private key. Since all incoming communications are being encrypted using the same algorithm, a common decryptor would therefore be used on the receiving end. Schneier further suggests that this is done so that someone listening in cannot recover the message (see Section 2.5).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the invention of the '501 application by using public-key cryptography for all communications to the receiver, as disclosed by Schneier, so that someone listening in cannot recover the message.

As per claim 2, 13, 22, 30, and 37, a digital signature written by the authority is disclosed (see claim 9).

As per claims 3, 14, 23, and 31, a certificate is generated (see claim 1).

As per claims 4, 15, 24, 32, and 38, mutual authentication is performed (see claim 8).

As per claim 5 and 25, the template is stored in the certificate (see claim 1).

As per claims 7 and 26, since the template is encrypted with the public key of the personal authentication system, it can only be decrypted by the personal authentication system.

As per claims 10 and 20, biometric or non-biometric information may be used (see claim 11).

As per claim 40, the method is executable on a program providing medium (see claim 27).

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Response to Arguments

18. Applicant's arguments, see Remarks, filed 16 March 2006, with respect to the rejections of claims 1-40 under 35 U.S.C. 102 and 103 have been fully considered and are persuasive in view of Applicant's amendments. Therefore, the rejection has been

withdrawn. However, upon further consideration, new grounds of rejection are made in view of the art cited above.

Conclusion

19. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew E. Heneghan, whose telephone number is (571) 272-3834. The examiner can normally be reached on Monday-Friday from 8:30 AM - 4:30 PM Eastern Time.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis-Jacques, can be reached at (571) 272-6962.

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
P.O. Box 1450
Alexandria, VA 22313-1450

Or faxed to:

(571) 273-3800

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

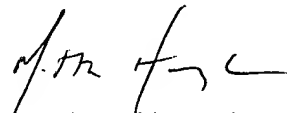
Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should

Art Unit: 2134

you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MEH

June 21, 2006

A handwritten signature in black ink, appearing to read 'M. Heneghan', written over a horizontal line.

Matthew Heneghan, USPTO Art Unit 2134